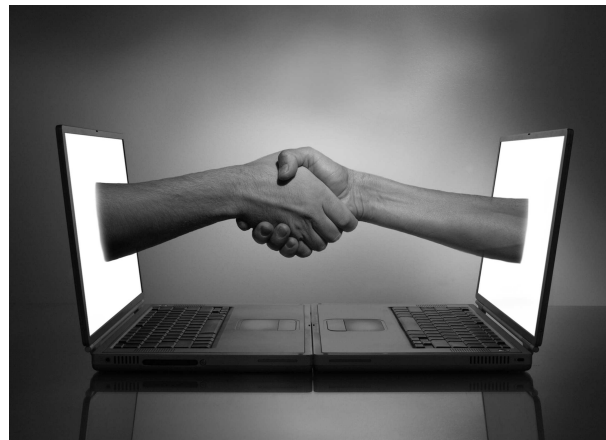




# TrustBuilder: Automated Trust Negotiation in Open Systems



Kent Seamons

Brigham Young University  
Internet Security Research Lab  
seamons@cs.byu.edu

3<sup>rd</sup> Annual PKI R&D Workshop, Gaithersburg, MD, April 12, 2004



# Outline

- ◆ Trust establishment in open systems
- ◆ Overview of trust negotiation
  - Sensitive credentials and access control policies
  - Research directions
- ◆ TrustBuilder
  - TLS-based trust negotiation protocol
- ◆ Future work



ISRL

Internet Security Research Lab  
BRIGHAM YOUNG  
UNIVERSITY

# Trust Negotiation Collaborators

## ◆ Theory

- M. Winslett, UIUC
- T. Yu, NCSU
- N. Li, Purdue
- W. Winsborough, GMU
- J. Mitchell, Stanford

## ◆ Systems

- K. Seamons, BYU
- C. Neuman, T. Ryutov, B. Tung, USC/ISI
- H. Orman, Purple Streak

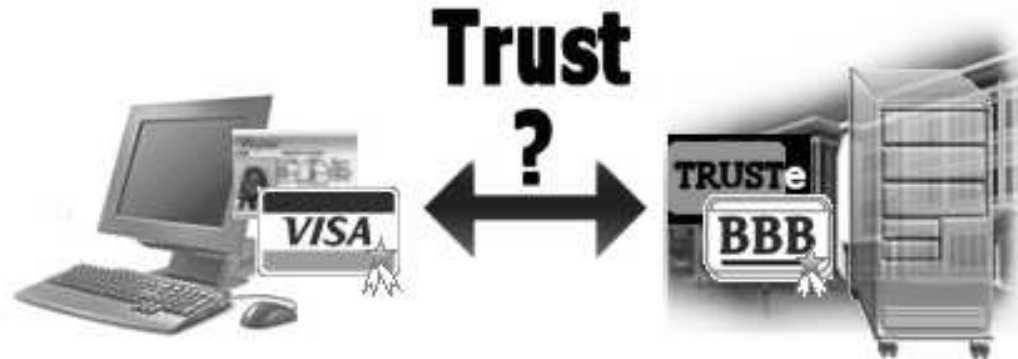
## ◆ Applications

- W. Nejdl, U. Hannover  
Educational consortia
- J. Basney, V. Welch, NCSA  
Grid computing

## ◆ Funding

- DARPA (Dynamic Coalitions Program)
- NSF (ITRs on TN, disaster response)
- Industry (ZoneLabs, Dallas Semiconductor, Network Associates Laboratories)

# Trust Establishment in Open Systems



- ◆ Problem: Identity is not relevant
- ◆ Solution: Access control decisions are based on attributes of both the client and server (mutual trust)
  - Client attributes: citizenship, security clearance, job classification, annual salary, affiliations, etc.
  - Server attributes: membership, privacy policy, customer satisfaction, result of recent security audit, etc.

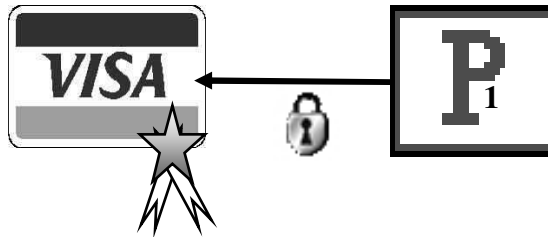
# Digital Credentials

- ◆ A credential is the vehicle for carrying attribute information reliably
- ◆ A credential contains attributes of the credential owner asserted by the issuer (attribute authority)
- ◆ Properties: verifiable and unforgeable



# Credentials Sensitivity

- ◆ Credentials may contain sensitive information and should be treated as protected resources





ISRL

Internet Security Research Lab  
BRIGHAM YOUNG  
UNIVERSITY

# Access Control Policies

- ◆ Credential disclosure is governed by an access control policy
  - Specifies credentials that must be received from another party prior to disclosing the sensitive credential to that party



ISRL

Internet Security Research Lab  
BRIGHAM YOUNG  
UNIVERSITY

# Trust Negotiation

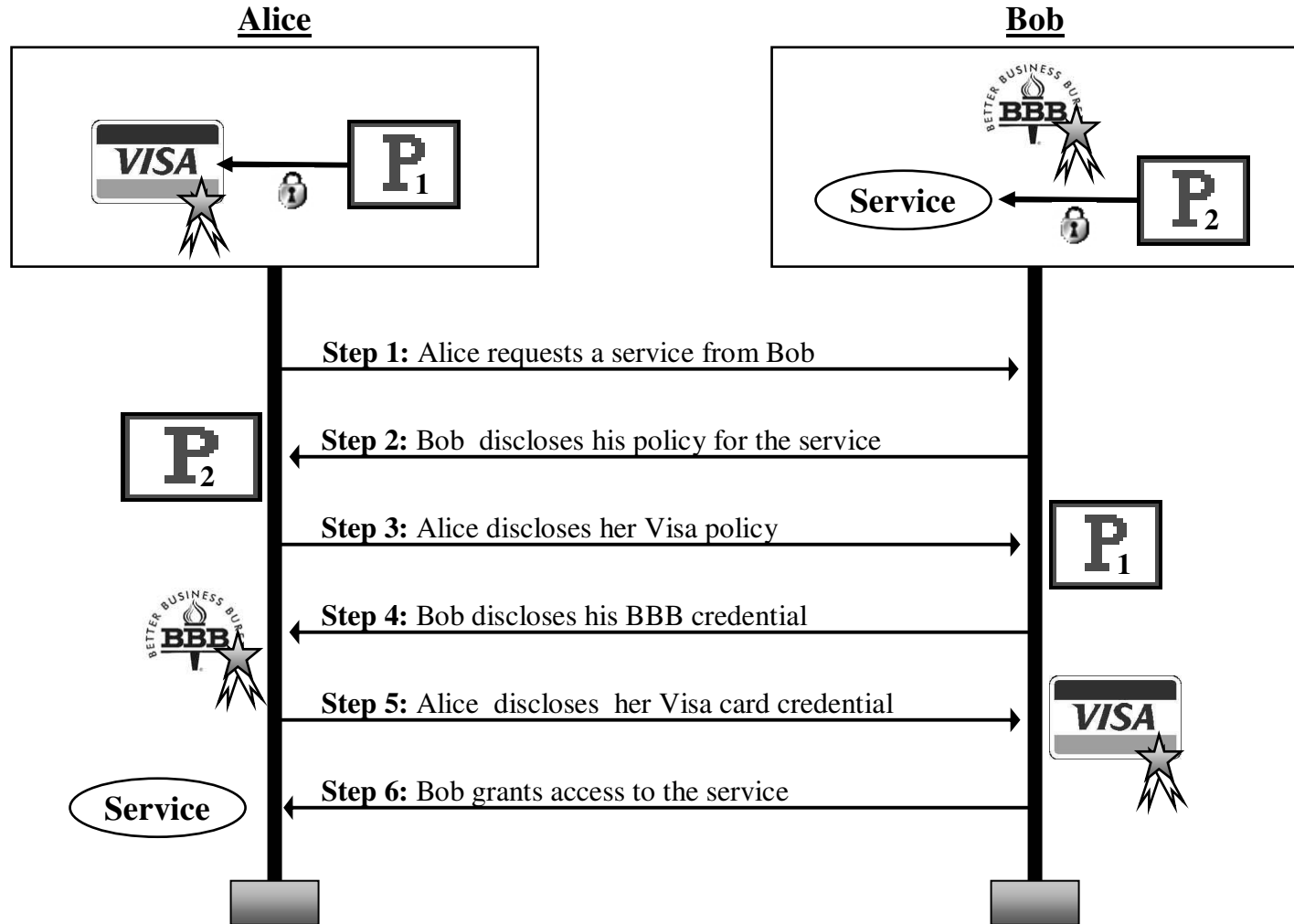
- ◆ The process of establishing trust between strangers in open systems based on the attributes of the participants



# Trust Negotiation Approaches

- ◆ Naïve:
  - Disclose all credentials with each request for service
- ◆ Trial and error
  - Disclose all credentials that are not sensitive, disclose sensitive credentials after required trust is established
- ◆ Informed
  - Disclose relevant policy first, then only disclose credentials necessary for a successful trust negotiation based on the trust requirements within the policy
- ◆ Advanced cryptography
  - Demonstrate attributes without disclosing credentials

# Trust Negotiation Example



# Research Directions

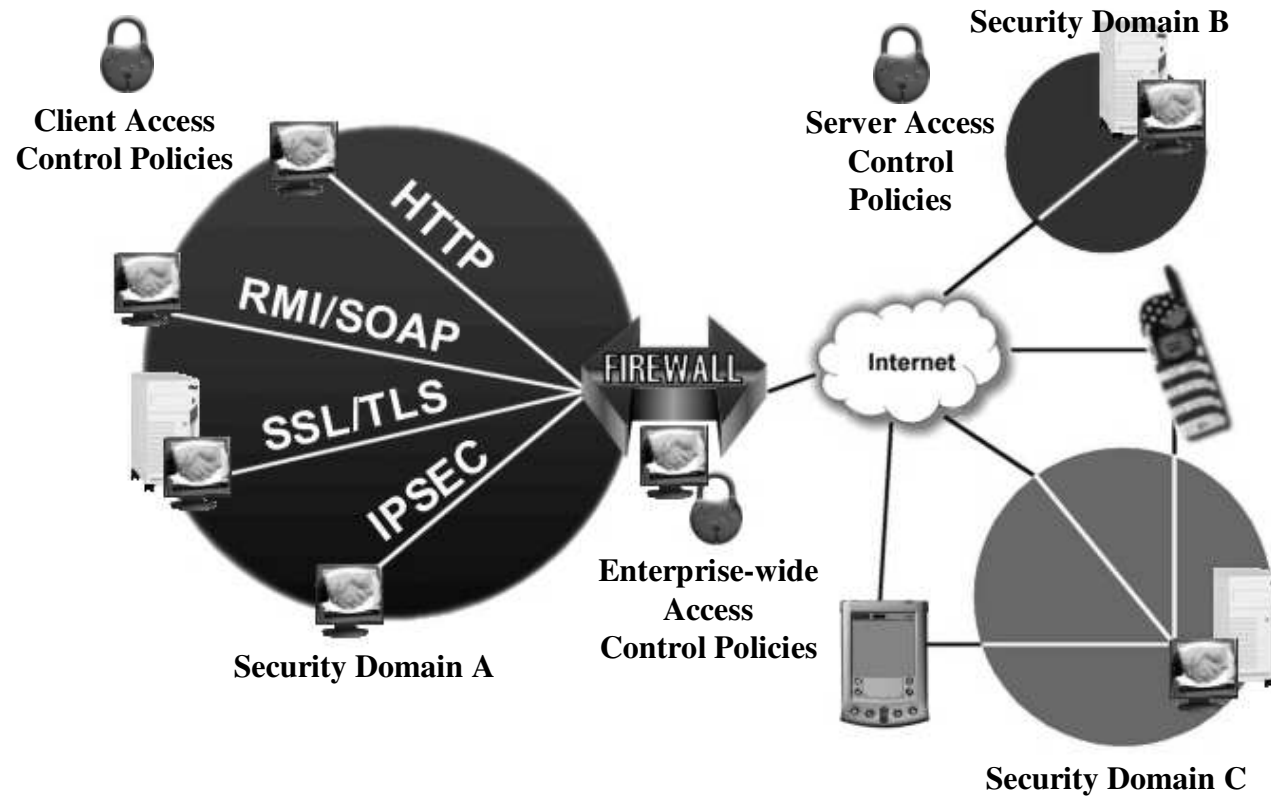
ISRL

Internet Security Research Lab  
BRIGHAM YOUNG  
UNIVERSITY

- ◆ Policy languages
  - Requirements (Seamons, Winslett – Policy 2002)
    - Compliance checker requirements
  - Policy language design
    - IBM TPL – (Herzberg et al., Oakland 2001)
    - RT - (Li, Mitchell, Winsborough, Oakland 2002)
      - Delegation of attribute authority, role mappings between organizations
    - PeerTrust (Nejdl et al., ESWS 2004)
  - Policy analysis tools (Li, Winsborough, Mitchell)
- ◆ Finding credentials at run time (Winsborough, Li)
- ◆ Preventing leaks/attacks during negotiation
  - Hidden credentials (Holt et al, WPES 2003)
  - OSBE (Li et al., PODC 2003)
  - Ack policies (Winsborough et al., Policy 2002)
  - Policy filtering (Yu et al.)
- ◆ Support for sensitive access control policies (Seamons, Winslett, Yu)
- ◆ Negotiation protocols & strategies
- ◆ Wireless and mobile device architecture for trust negotiation – surrogate TN
- ◆ Testbed implementations - HTTPS, TLS, content-triggered TN, ...

# TrustBuilder Architecture

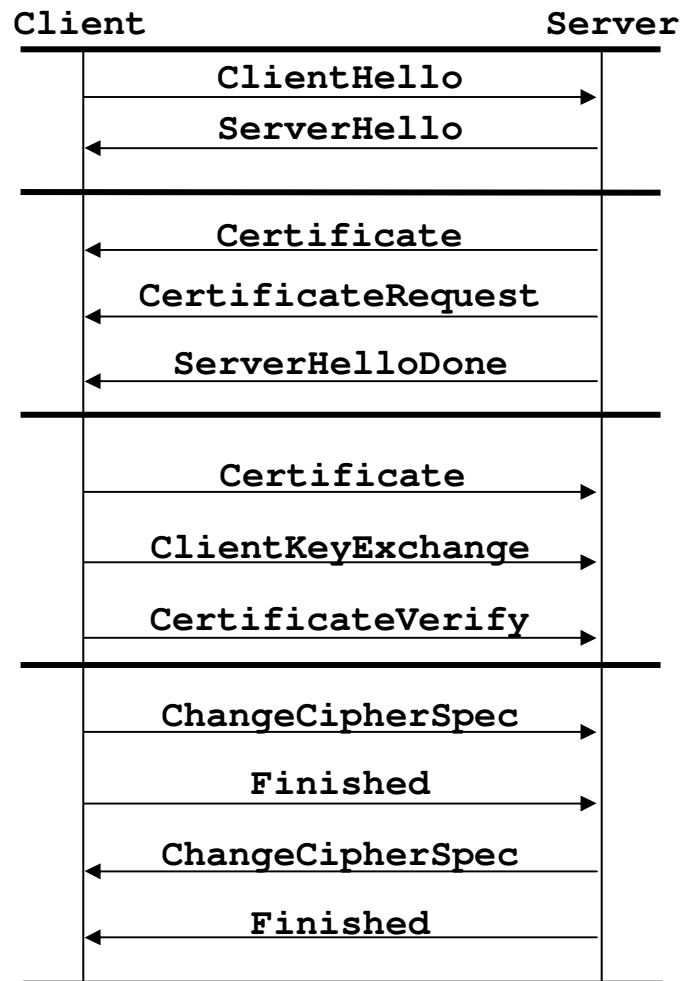
- ◆ Goal – Ubiquitous trust negotiation
- ◆ TrustBuilder integrates into existing Internet technologies
  - Current Deployments - HTTPS, TLS, SSH, SMTP



# Trust Negotiation in TLS (TNT)

- ◆ TLS-based protocol for trust negotiation
- ◆ Resulted from an analysis of the SSL/TLS handshake protocol for its suitability as a protocol for trust negotiation
  - TLS provides an option for client/server authentication using certificates
  - Goal: extend TLS client/server authentication to support trust negotiation

# TLS Handshake Protocol using RSA Key Exchange



# Limitations of TLS for Establishing Trust between Strangers

- Certificates are exchanged in plain text
- Client and server each disclose only one certificate chain
- Server can specify a list of trusted certifying authorities; client cannot
- Server always discloses its certificate first
- Server certificate ownership is not yet established when the client discloses its certificate

# Extend TLS Authentication to Support Trust Negotiation

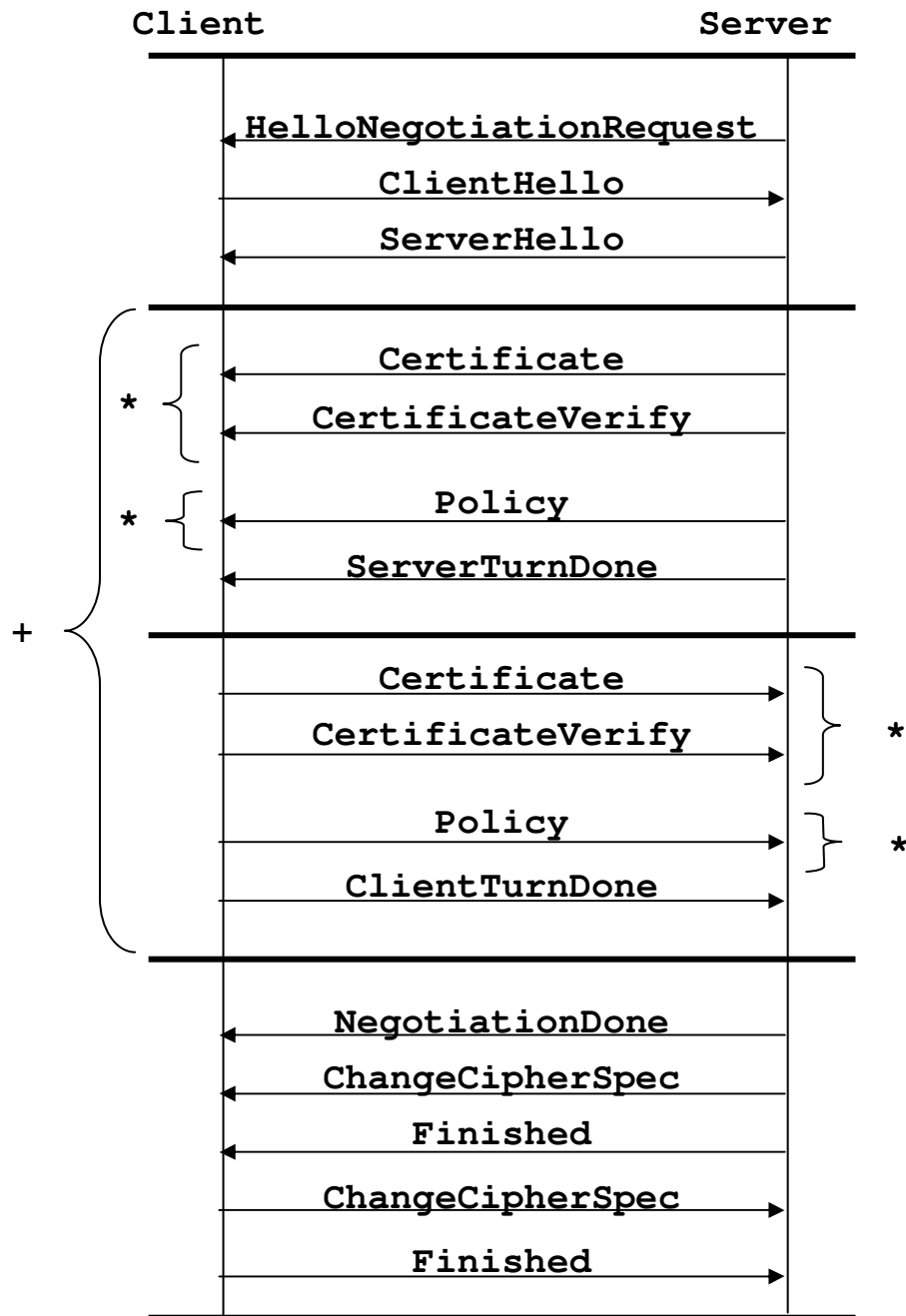
- ◆ Extend the TLS handshake protocol to function as a trust negotiation protocol
- ◆ TNT leverages existing and proposed features of the TLS handshake protocol
  - Client hello and server hello extensions
  - TLS rehandshake
  - Session resumption

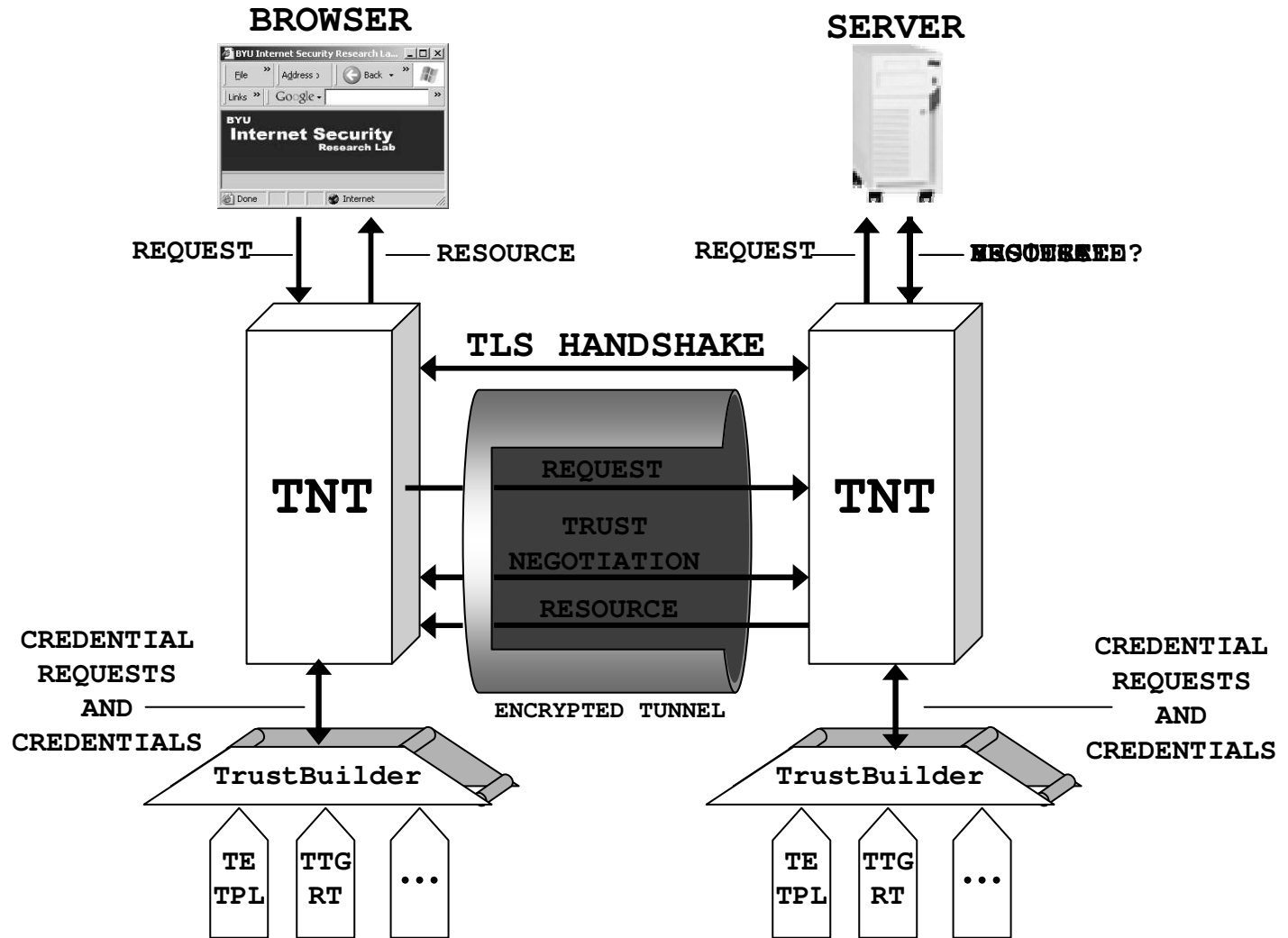
# TLS Rehandshake

- ◆ In the context of an encrypted TLS session, either the client or the server may initiate a rehandshake.
  - The server desires further certificates from the client for purposes of authentication or authorization.
  - Cipher suite upgrading
  - Replenishment of keying material
- ◆ Trust negotiations involving sensitive credentials and policies must be conducted over a secure channel in order to remain confidential. The initial TLS handshake is not confidential.
- ◆ TNT is designed to occur in the context of a TLS rehandshake.

# TNT Protocol

Overview:





# TNT Implementation

- ◆ A prototype of TNT has been developed for the TrustBuilder architecture
  - TNT implementation is an extension to the Java PureTLS toolkit developed by Eric Rescorla (see <http://www.rftm.com/>)
  - Policy language and compliance checker is built using the IBM Trust Establishment system developed at the IBM Haifa Research Lab (RSA Security Conference 2001)

# Future work

- ◆ Integrate emerging trust negotiation policy languages (RT, PeerTrust) into TNT to determine if the protocol is general purpose
- ◆ Policy creation tools
- ◆ Requirements for real-world applications
  - Grid computing, Semantic Web
- ◆ Privacy protection during trust negotiation
- ◆ Trust negotiation in Kerberos PK-INIT
- ◆ Architectures for mobile devices – surrogate trust negotiation



ISRL

Internet Security Research Lab  
BRIGHAM YOUNG  
UNIVERSITY